

N i e d e r s c h r i f t

über die gemeinsame - öffentliche - Sitzung des Ausschusses für Inneres und Sport (111. Sitzung, erster Teil¹) und des Ausschusses für Rechts- und Verfassungsfragen (88. Sitzung)

am 20. August 2026

Hannover, Landtagsgebäude

Tagesordnung:

Seite

31. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Niedersachsen für das Jahr 2025

Unterrichtung - [Drs. 19/11151](#)

<i>Vorstellung des Berichts</i>	3
<i>Aussprache</i>	10
<i>Verfahrensfragen.....</i>	23

¹ Über den zweiten Teil der Sitzung des Ausschusses für Inneres und Sport wird eine gesonderte Niederschrift erstellt.

Anwesend:

Mitglieder des Ausschusses für Inneres und Sport:

1. Abg. Doris Schröder-Köpf (SPD), Vorsitzende
2. Abg. Deniz Kurku (SPD)
3. Abg. Alexander Saade (SPD)
4. Abg. Julius Schneider (SPD)
5. Abg. Ulrich Watermann (SPD)
6. Abg. Rüdiger Kauroff (i. V. des Abg. Sebastian Zinke) (SPD)
7. Abg. André Bock (CDU)
8. Abg. Saskia Buschmann (CDU)
9. Abg. Birgit Butter (CDU)
10. Abg. Lara Evers (CDU)
11. Abg. Alexander Wille (CDU)
12. Abg. Michael Lühmann (GRÜNE)
13. Abg. Nadja Weippert (GRÜNE)
14. Abg. Stephan Bothe (AfD)

Mitglieder Ausschusses für Rechts- und Verfassungsfragen:

1. Abg. Christoph Plett (CDU), Vorsitzender
2. Abg. Wiebke Osigus (SPD)
3. Abg. Julius Schneider (SPD)
4. Abg. Evrim Camuz (GRÜNE)
5. Abg. Thorsten Paul Moriß (AfD)

Als ZuhörerIn oder Zuhörer (§ 94 GO LT):

Abg. Christoph Willeke (SPD).

Von der Landtagsverwaltung:

Regierungsrat Biela,
Beschäftigte Geerts.

Niederschrift:

Regierungsdirektor Dr. Bäse,
Oberregierungsrätin Harmening, Stenografischer Dienst.

Sitzungsdauer: 10:00 Uhr bis 11:46 Uhr.

Tagesordnung:

31. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz Niedersachsen für das Jahr 2025

Unterrichtung - [Drs. 19/11151](#)

gemäß § 62 Abs. 1 GO LT überwiesen am 14.07.2026

federführend: AfluS

mitberatend: AfRuV

Vorstellung des Berichts

LfD **Lehmkemper**: Vielen Dank, dass ich die Gelegenheit erhalte, den 31. Bericht des Landesbeauftragten für den Datenschutz vorzustellen. Heute übernehme ich diese Vorstellung zum dritten Mal.

In den zurückliegenden Jahren haben wir den Jahresbericht immer vor der Sommerpause vorgestellt und uns dabei auf das Berichtsjahr fokussiert. Jetzt ist die Zeit im Jahr vorangeschritten, und wir stellen ihn in einer gemeinsamen Sitzung von Innen- und Rechtsausschuss vor. Wir haben Ihnen den Bericht bereits zum eigentlich vorgesehenen Termin für die Vorstellung zugesandt. Damit haben wir auf einen Wunsch Ihrerseits reagiert, damit die Möglichkeit besteht, sich besser auf die Vorstellung vorzubereiten.

In dem Bericht haben wir aktuelle Bezüge in den Vordergrund gestellt. Er ist auch etwas kompakter abgefasst worden als in den vergangenen Jahren. Dabei haben wir uns auf Aktuelles fokussiert, weshalb der Jahresbericht zwar seitenmäßig dünner als die Jahre zuvor ausfällt, inhaltlich aber auf keinen Fall.

Im Jahr 2025 haben mein Team - über 50 Datenschutzexpertinnen und -experten - und ich viel getan, viel versucht, und einiges ist auch gelungen, um die Datenschutzthemen in Niedersachsen den Bürgerinnen und Bürgern, Ihnen in der Politik und auch den niedersächsischen Unternehmen näherzubringen.

Ich möchte heute gern einige herausgehobene Themen und Einzelfälle mit Ihnen besprechen.

Das Thema, das uns im Moment wohl alle sehr bewegt, sind die Kommunalwahlen am 13. September 2026, die auch die Behörde sehr bewegen; denn Wahlen beschäftigen uns immer sehr. Da gibt es immer eine gewisse Häufung an Fragen, wozu wir kürzlich auch eine Pressemitteilung herausgegeben haben. Dort geht es zum Beispiel um die Frage, wie die Parteien an die Daten der Wählerinnen und Wähler kommen. Dazu gibt es eine Regelung im Bundesmeldegesetz; das alles ist also rechtmäßig, und die Parteien halten sich in aller Regel auch daran.

Es gibt aber eine Besonderheit, die ich nicht unerwähnt lassen möchte: Diese Kommunalwahl ist die erste Wahl in Niedersachsen, in der die EU-Verordnung über die Transparenz und das Targeting für politische Werbung, die TTPW-Verordnung, anwendbar ist. Sie sehen das praktisch an den QR-Codes, die auf den großen Aufstellplakaten angebracht sind. Die TTPW-Verordnung sieht vor, dass die Finanzierung der Wahlwerbung offengelegt wird, zumindest im kommerziellen Bereich. Dazu gibt es mehrere Handreichungen. Ich habe bei einer der größeren politischen

Parteien dazu schon einmal einen Vortrag gehalten. Bei den Laternenmastplakaten, die fast ausschließlich von Ehrenamtlichen bezahlt und aufgehängt werden, kann man auf die QR-Codes und den entsprechenden Nachweis verzichten. Auch wenn ich selbst nie Plakate aufgehängt habe, weiß ich noch, wie aufwendig es ist, so etwas zu organisieren. An dieser Stelle wollte auch die EU dem Ehrenamt entgegenkommen.

Ich gehe auf die TTPW-Verordnung so ausführlich ein, weil sie, glaube ich, ein wirklich gutes Instrument ist, um die Beeinflussung von Wahlen zumindest einzudämmen; denn heutzutage können politische Akteure - manchmal auch ausländische „Mächte“, wie der Bundesinnenminister sagte - gerade im Internet große Reichweiten erreichen. Zum einen möchte man wissen, wie eine Kampagne finanziert wird; ich meine, darauf hat der mündige Bürger ein Recht. Zum anderen ergibt sich daraus eine Einschränkung: Personalisierte Werbung im Sinne von „Du hast dir diese oder jene Website angeschaut, weshalb dich diese oder jene politische Richtung interessiert“ ist genauso untersagt wie Onlinewerbung, die aufgrund der Zugehörigkeit zu einer religiösen oder ethnischen Gruppe etc. ausgespielt wird. Das ist richtig! Ich halte es für ein wesentliches Merkmal der politischen Meinungsbildung, dass darauf auch und gerade im Online-Bereich geachtet wird.

Zu diesem Thema gehen bereits Beschwerden ein; natürlich noch nicht in großer Anzahl. Aber wir befassen uns intensiv damit. Ich möchte Sie ermuntern: Wenn Sie dazu Fragen haben, wenn Ihnen etwas komisch vorkommt - wir fühlen uns dafür zuständig. Wir halten es für einen Dienst an diesem Staat, darauf zu reagieren, und wir machen das gern.

Ein weiteres Thema im Zusammenhang mit den Wahlen möchte ich kurz ansprechen, auch wenn ich bedauerlicherweise nicht originär zuständig bin: KI in Wahlwerbung, insbesondere auf Wahlplakaten. Wir haben bereits mehrere Beschwerden zum Einsatz von KI auf Wahlplakaten und in Internetveröffentlichungen. Ich möchte Sie alle aufrufen: Seien Sie damit vorsichtig! Die Macht der Bilder ist eine andere als die des Wortes. Man kann mit Bildern andere Effekte erzielen. Auch wenn das kurzfristig sinnvoll sein kann, so glaube ich doch, dass das auf die Dauer schwierig wird.

Wir sind dafür aber nicht zuständig, wie der Bund entschieden hat. Zuständig ist die Bundesnetzagentur. Ich gebe alles, was dazu bei uns eingeht, mit Nachdruck dorthin ab und weise darauf hin, dass ich wünsche, dass diese Hinweise verfolgt werden. Ich mache keinen Hehl daraus: Ich hätte diese Zuständigkeit gern erhalten, ebenso wie meine Kolleginnen und Kollegen in den anderen Ländern auch, denn bei Kommunal- und Landtagswahlen wäre es vermutlich effizienter gewesen, direkt an die Landeswahlleitung heranzutreten, um solchem KI-Einsatz entgegenzutreten. Aber diese Möglichkeit habe ich nicht. Trotzdem möchte ich darauf hinweisen, und ich sehe an dieser Stelle ein Problem.

Damit komme ich zum nächsten Thema, das ich Ihnen vorstellen möchte: künstliche Intelligenz. Da sehe ich aber nicht überall Probleme. In dem Bereich haben wir bereits eine ganze Menge getan. Ich habe Ihnen bereits im vergangenen Jahr berichtet, dass wir eine Stabsstelle für künstliche Intelligenz eingerichtet haben, deren Kompetenz sehr gut abgefragt und genutzt wird, auch von den Landesbehörden. Wir haben uns zum Beispiel mit der Implementierung von LLMoin, dem aus Hamburg stammenden Chatbot der Landesregierung, befasst, der „nachgenutzt“ wird. Wir haben dazu - ich glaube, bundesweit erstmalig - das viel beschriebene Prinzip „einer prüft für alle“ angewendet. Das heißt, der Hamburger Kollege Fuchs hat sich LLMoin genau angeschaut, und wir haben im Prinzip dessen Prüfungsergebnis übernommen und nur

Landesspezifika dem Innenministerium ins Stammbuch geschrieben. Hamburg hat bereits eine Rechtsgrundlage für Einsatz und Nutzung, Niedersachsen noch nicht. Das haben wir dem MI natürlich mit auf den Weg gegeben.

Wir schauen uns, wie Hamburg auch, fortlaufend den Systemprompt an und sorgen dafür, dass das System gehärtet wird. Von daher sind wir mit unserem Verfahren, mit unserer Prüfung und mit unseren Ergebnissen noch nicht fertig, stehen aber im dauernden Austausch. Das läuft seit einiger Zeit richtig gut, weil man hoffentlich erkannt hat, dass wir eine konstruktiv-kritische Rolle spielen, die der Sache hilft. Denn wohl niemand hat etwas davon, wenn alle möglichen KI-Modelle frei Hand eingesetzt werden und dann auf einmal niedersächsische Daten in China oder sonst wo in der Welt auftauchen. Wir sollten also auf dieses Thema achten.

Da einige von Ihnen dankenswerterweise anwesend waren, möchte ich auf unser KI-Symposium hinweisen, das wir im November 2025 im Forum des Landtags durchgeführt haben. Wir haben fast durchweg positive Rückmeldungen zu dieser Art von Veranstaltung bekommen und haben uns vorgenommen, so etwas zu spannenden Themen mal wieder zu machen; einen entsprechenden Bedarf scheint es zu geben. Zu Beginn der Veranstaltung hatte ich mich gefragt, ob sich alle 150 Teilnehmerinnen und Teilnehmer der Tatsache bewusst waren, dass sie beim Datenschutz zu Gast waren. Aber das wurde mir immer wieder bestätigt. Von daher glaube ich, dass dies ein Teil der Arbeit sein wird, die in den nächsten Jahren ansteht.

Ein Wunsch ist immer wieder an uns herangetragen worden: der nach Rechtssicherheit. Das bedeutet für Sie: Schaffen Sie Rechtsgrundlagen! Seien Sie mutig, und zwar auch für Bereiche, für die die Felder noch nicht bestellt sind, für die man nicht vom Nachbarland Regelungen übernehmen kann! Setzen Sie sich in dieser Diskussion mit uns auseinander. Ein Teil der Arbeit wird derzeit über die beiden Omnibus-Gesetzgebungsverfahren auf der EU-Ebene erledigt. Aber keine Sorge: Auch auf der Landesebene bleibt für Sie hinsichtlich der Rechtsgrundlage noch genug zu tun.

Hierzu liegt ein erster Entwurf des NDIG vor, zu dem wir Stellung genommen haben. Später wird dieser Gesetzentwurf sicherlich in beiden Ausschüssen behandelt. Ich bin zuversichtlich, dass wir vorankommen und in die Richtung des rechtlichen Stands von Hamburg kommen, was KI angeht. Wir werden diesen Prozess weiterhin intensiv begleiten. Nutzen Sie unsere Kompetenz! Datenschützer sind zwar nicht immer angenehme Gesprächspartner - und manchmal werden wir uns auch nicht einig -, aber in den zurückliegenden drei Jahren habe ich immer den Eindruck gehabt: Wir sind durch den Austausch mit Ihnen schlauer geworden. Und wir haben die Hoffnung, dass auch Sie alle durch den Austausch mit uns schlauer werden.

Wie im vergangenen Jahr möchte ich das Thema der KI-Marktüberwachung ansprechen. Hierzu wurde mittlerweile entschieden, dass diese Aufgabe für die nicht öffentlichen Stellen - Unternehmen und dergleichen - seit dem 2. August dieses Jahres von der Bundesnetzagentur wahrgenommen werden muss. Hingegen ist noch nicht entschieden, wer die KI-Marktüberwachung für die öffentlichen Stellen übernimmt. Mit etwas Verwunderung sehe ich, dass viele Länder - dazu gehört leider auch Niedersachsen - kein wirkliches Interesse an dieser Aufgabe haben. Würde man auch diese Aufgabe der Bundesnetzagentur zuweisen, hätte das zur Konsequenz, dass ein KI-Modell, das bei den Schulen oder bei der Polizei eingeführt wird, vom Bund überprüft wird. Mit Blick auf den Staatsaufbau habe ich im Studium gelernt, dass die Länder tun sollen, was den Ländern ist. Ich will nicht sagen, dass das einfacher oder schwieriger ist. Aber es kann

sich bisweilen ein Vorteil bei der Ausbuchstabierung bestimmter Themen ergeben, wenn man nur bis zur Prinzenstraße und nicht bis nach Bonn muss.

Mehr will ich dazu nicht sagen. Wir würden die Aufgabe der KI-Marktüberwachung im öffentlichen Bereich sehr gern übernehmen, aber nicht, um eine besondere Bürokratie aufzubauen. Ich habe eher den Eindruck, dass die besondere Bürokratie die Bundesnetzagentur ist, weil sie in ihren Zuständigkeiten ausufert. Als überzeugter Föderalist möchte ich es deutlich ausdrücken: Ich habe nur wenig gesehen, was besser wurde, weil nur der Bund es gemacht hat. Vielmehr habe ich das Zusammenspiel zwischen Bund und Ländern als in aller Regel förderlich erlebt.

Ein ganz anderes Thema: Wir haben viel zu tun. Das trifft sicherlich auf alle Landesdatenschutzbeauftragten zu, die hier vorgetragen haben. Klar ist aber, dass alle Datenschutzbehörden im zurückliegenden Jahr 2025 einen erstaunlichen Anstieg der Zahl der Beschwerden feststellen konnten - mit 70 % gegenüber 2024 auf etwas mehr als 4 000 so deutlich, dass ich es nicht unerwähnt lassen möchte. Zum Teil liegt das sicherlich an KI, wie ich in diesem Kreis schon einmal vorgetragen habe. Mithilfe von KI können Beschwerden viel schneller als früher verfasst werden, denn man muss sich nicht mehr durch eine Handvoll etwas langatmiger Webseiten arbeiten. Im ersten Halbjahr 2026 sind bei uns bereits 2 860 Beschwerden eingegangen, sodass wir für das Jahr 2026 mit mehr als 6 000 Beschwerden rechnen.

Sie alle hätten es mitbekommen, wenn der Landesbeauftragte für den Datenschutz auch 70 % mehr Personal bekommen hätte. Das ist unrealistisch, völlig klar! Aber wir haben das Limit, das für die Beschwerdebearbeitung besteht, überschritten. Das erleben auch Sie mitunter, weil einige der Beschwerdeführer Petitionen einreichen, weil es kein anderes Mittel gibt. Und wir merken, dass wir lange brauchen. Laut DSGVO haben wir nicht die Möglichkeit, bestimmte Fallkonstellationen nicht zu betrachten. Deshalb müssen wir uns mit jeder Beschwerde inhaltlich befassen. Und die Gerichte fangen allmählich an, uns ein Entschließungsermessen bezüglich der Wahl der Maßnahme einzuräumen. Wir gehen damit, was unsere Seite betrifft, so um, dass wir Fallgruppen bilden und bestimmte Vorgänge nur noch mit Hinweisschreiben bearbeiten, im Zweifelsfall mit besonders qualifizierten Hinweisschreiben. Aber wir öffnen uns auch in einer Weise für technische Möglichkeiten, wie wir das bislang nicht gemacht haben. Zusammen mit dem IT.N haben wir ein Geschäftsprozessmanagement angestoßen und wollen so weit wie möglich digitalisieren und automatisieren. Das ist für eine Datenschutzbehörde allerdings eine besondere Herausforderung - denn wenn wir es nicht richtig machen, dann gibt es wohl niemanden, der es richtig macht. Das setzt dem KI-Einsatz im Moment gewisse Grenzen, auch wenn ich perspektivisch zu einem KI-Einsatz kommen möchte. Aber das ist nicht so ganz einfach und bindet zusätzlich zu den Beschwerdezahlen Ressourcen, die aber gut genutzt werden.

Zur Verdeutlichung: Im Jahr 2022 gingen bei uns 2 058 Beschwerden ein. Bis Ende 2026 werden wir mindestens von einer Verdreifachung sprechen, ohne dass wir über dreimal so viel Personal verfügen. Aber ich habe ein tolles Team in meinem Haus. Und wir versuchen, bei Neubesetzungen attraktive Arbeitsplätze zu bieten. Das ist entscheidend. Wenn sich herumsprechen sollte, dass man von Akten erschlagen wird, wenn man nur die Bürotür öffnet, dann sind die Dienstposten und Arbeitsplätze nicht wirklich attraktiv. Von daher müssen wir bestrebt sein, einen attraktiven und spannenden Aufgabenmix zu erhalten. Das macht mir als Verantwortlicher für meine Datenschützerinnen und -schützer manchmal ernsthafte Sorgen. Ich habe allen versprochen - und das wiederhole ich hier gern -: Ich habe ein breites Kreuz. Die einzigen, die mich abwählen können, sind Sie. Und solange ich mein Amt ausfülle, bearbeiten wir die Beschwerden in gewisser Weise nach Dringlichkeit: Steht hinter dieser Beschwerde ein großer Verstoß gegen das

Datenschutzrecht? Oder genügt es, wenn wir darauf hinweisen, dass man etwas besser auf einem anderen Weg macht? Aber es gibt diese großen Datenschutzvorfälle! Auf sie müssen wir eingehen. Die wirklich wichtigen Dinge wollen wir vorantreiben.

All das, was ich Ihnen vorgetragen habe, sieht man am Thema Videoüberwachung sehr deutlich. Wir hatten im Jahr 2025 750 Fälle in diesem Bereich.

Das sind ganz häufig Fälle, bei denen sich Leute an der Videokamera im nachbarlichen Garten, an der Wildkamera im Wald oder an der Dashcam des vorausfahrenden oder nachfolgenden Fahrzeugs stören. Hierzu habe ich einen kuriosen Fall aus einem anderen Bundesland gehört: Jemand hat sich beschwert, dass er über eine Strecke von 150 km von der Dashcam eines vorausfahrenden Autos aufgezeichnet wurde. Das ist ohne Zweifel ein Datenschutzverstoß. Aber manchmal hilft der Selbstschutz: Wenn man nicht unbedingt hinter dem Auto mit der Dashcam fahren muss, kann man selbst viel dazu beitragen, den Datenschutzverstoß für sich selbst in Grenzen zu halten.

Aber es gibt im Bereich der Videoüberwachung auch andere Fälle, die bei mir ein ernstes Störgefühl auslösen. Das sind häufig Fälle, bei denen Unternehmen Mitarbeiterinnen und Mitarbeiter sehr gezielt überwachen oder bei denen in Fitness-Studios Bereiche mit dem Hinweis auf einen Diebstahlschutz überwacht werden, obwohl diese Überwachung zu weit geht. Solche Fälle schauen wir uns intensiv an.

Wo etwas falsch läuft, merken wir regelmäßig bei Prüfungen. Wir haben im Jahr 2025 an einer bundesweit koordinierten und angekündigten Prüfung teilgenommen, bei der es nicht nur um allgemeine Videoüberwachungen und Ähnliches ging, sondern wir haben uns zusammen mit Polizei, Zoll und kommunalen Stellen bestimmte Schwerpunkte angeschaut: Spielhallen, Kioske, Cafés, Shisha-Bars, Tankstellen. Auch dort haben wir Videoüberwachungssysteme vorgefunden, bei denen schon die einfachsten Basics wie die Ausschilderung nicht erfüllt waren. In solchen Fällen sind Bußgelder verhängt worden.

Dazu zählte neben den genannten Betrieben auch ein Logistikunternehmen, das Kunden und Beschäftigte überwachte; Näheres können Sie dem Tätigkeitsbericht ab Seite 80 entnehmen. So kommt dann die Datenschutzaufsicht zu ihren praktischen Fällen, in denen wir einschreiten wollen und müssen. Insgesamt haben wir 34 Bußgelderstbescheide erlassen und Bußgelder in Höhe von 705 000 Euro verhängt.

Das höchste Bußgeld sticht dabei heraus: 485 000 Euro gegen ein Kreditinstitut, das Kundendaten im Zahlungsverkehr mit zugekauften Daten gemischt und daraus Kenntnisse für Werbung und Weiteres gezogen hat. Über diese Fälle hatte ich auch in den zurückliegenden Jahren berichtet. Diese Smart-Data-Fälle stammen aus der Zeit, bevor ich das Amt angetreten habe. Es handelte sich ursprünglich um rund 30 Fälle, und der von mir genannte ist der letzte davon. In fast allen anderen Fällen sind wir zu einer gütlichen Verständigung gekommen. Diese Fälle haben mir und auch manchen von Ihnen erhebliche Sorgen bereitet. Von daher freut es mich besonders, dass ich zu den Smart-Data-Fällen berichten kann, dass wir im Verlauf von zwei Jahren weitgehend hinter den Kulissen - das war viel Arbeit für die Kolleginnen und Kollegen; übrigens unter Beteiligung einiger Abgeordneter, die heute hier aber nicht anwesend sind - versucht haben, eine Lösung für diese Bankengruppe für die Zukunft zu finden. Zusammen mit ihr ist es uns gelungen, ein Einwilligungsmanagement für die Datenverarbeitung aufzubauen, das gänzlich ohne Tricks, ohne besonders große Buttons, ohne Dark Patterns und ohne andere ähnliche

Elemente auskommt. Das liegt auch im Interesse der Banken, weil sie mit diesem Verfahren, wie sie selbst sagen, zukunftsicher arbeiten können. Dieses Verfahren soll zunächst ab dem Sommer 2026 in Niedersachsen ausgerollt werden. Vielleicht macht es Schule; denn so stelle ich mir die Arbeit auch in derart hakeligen Bereichen wie der Datenerhebung vor. Denn uns allen ist völlig klar, dass heute mit Daten auch ein Geschäft gemacht wird. Das muss auch so sein. Aber die Datenschutzgrundsätze müssen dabei eingehalten werden. Aus meiner Sicht ist das ein schönes Ergebnis.

Ein weiterer großer Bereich umfasst die Cybersicherheit und die Meldung von Datenpannen. Seine Bedeutung nimmt im Jahr 2026 gegenüber dem Vorjahr deutlich zu. Mit 1 607 Fällen hatten wir im Berichtsjahr einen nur leichten Anstieg gegenüber 2024 zu verzeichnen, was dem Trend der Vorjahre entspricht. Aber im ersten Halbjahr 2026 verzeichnen wir bereits 1 245 Fälle. Wir sehen also einen deutlichen Anstieg, der alle Teilbereiche umfasst. Wir wissen noch nicht im Einzelnen, was zu diesem Anstieg führt. Aber ich glaube, dass dieser Bereich in der Bevölkerung sehr präsent ist. Das spricht für eine hohe Sensibilisierung - das ist gut! Wir stellen infolge der Vernetzung fest, dass es Fälle gibt, in denen es gleich eine Vielzahl von Betroffenen gibt, die Datenpannenmeldungen zum gleichen Sachverhalt abgeben.

Hierzu möchte ich ein in der Presse nicht sonderlich präsent Beispiel nennen: Ein Dienstleister für Berufsfotografen mit Sitz außerhalb von Niedersachsen hatte eine größere Datenpanne. Allein bei uns gingen 50 Datenpannenmeldungen ein, weil 50 niedersächsische professionelle Fotografen an diesen Dienstleister angeschlossen sind. So ergeben sich schnell große Zahlen. Die Landesdatenschutzbeauftragten haben sich zu mehreren Beispielen bundesweit koordiniert und versuchen, ihren Teil der Arbeit bundesweit koordiniert zu erledigen, so auch in dem im Innenausschuss einmal thematisierten Datenschutzvorfall der Ameos-Kliniken.

Auch wenn Ameos ein schweizerisches Unternehmen ist und die DSGVO dort nicht gilt - wirklich schlecht ist der Datenschutz auch dort nicht -, so waren doch vier oder fünf niedersächsische Kliniken betroffen. Inzwischen konnte nach viel Kleinarbeit von Ameos bestätigt werden, dass keine Patientendaten aus niedersächsischen Kliniken abgeflossen sind. Diesen Vorgang haben die Kollegen in Sachsen-Anhalt koordiniert, weil dort die erste Datenschutzmeldung dazu einging, aber auch wir waren sehr intensiv beteiligt. Dass die Zahl der Datenpannen zunimmt, scheint mir recht einfach zu erklären zu sein, denn der Umfang der Datenverarbeitung nimmt zu. Ich habe einmal gelesen, dass man zu dem Zeitpunkt, als man anfang, die DSGVO zu konzipieren, von rund zehn Datenverarbeitungsvorgängen je Bürger und Tag ausgegangen ist. Nehmen Sie mal Ihr Smartphone zur Hand - dann sind sie vermutlich jetzt beim Hundertfachen. Auch wenn das alles erklärbar ist, macht es das nicht besser. Wir haben die Pflicht zum Datenschutz, und diese müssen wir gerade auch in der jetzigen geopolitischen Lage ernst nehmen. Von daher sind Datenpannen und Cybervorfälle in unserem Fokus, und wir kümmern uns darum.

Ein weiteres wichtiges Thema ist bei uns die Schule insgesamt. Ich erwähne es an dieser Stelle, weil wir den Eindruck haben, dass im Bereich Schule noch viel zu tun ist, um die Datensicherheit herzustellen. Wir begrüßen es aus Datenschutzsicht ausdrücklich, dass zukünftig in Niedersachsen ab der 7. Klasse landesweit Tablets bereitgestellt werden. Aber erstens wird es noch eine Weile dauern, bis von der 7. Klasse an bis zur 13. Jahrgangsstufe alle versorgt sind. Wir haben also noch eine Weile die wirklich unbefriedigende Situation, dass private Endgeräte irgendwie in öffentliche Netzwerke eingebunden werden müssen, was ein Sicherheits- und Datenschutzproblem ist. Zweitens hören wir von allen Seiten, auch von den Kommunen, dass mehr Guidance benötigt werde, also mehr Anleitung und mehr Hinweise vom zuständigen Ressort.

So wäre zu klären, welche Apps auf diesen Tablets installiert werden dürfen. Ein Beispiel: Mein Sohn hat im Zuge seiner Ausbildung bei einem größeren Unternehmen ein Tablet erhalten, auf das er sich aber nur Apps ziehen darf, die das Unternehmen über eine Whitelist freigegeben hat. Wenn man also Tablets in ein Schulnetzwerk einbindet, müsste es eine entsprechende technische Lösung geben, die nach meinem Eindruck - bei aller Wertschätzung für die pädagogische Freiheit der Schulen - zentral vorgegeben ist. Das kann dann nicht jede Schule für sich regeln.

Im Schulbereich gibt es also noch sehr viele Themen. Wir stehen dazu im Austausch. Das läuft. Wir geben die Hoffnung nicht auf und werden weiter daran arbeiten.

Auf den Bereich, der über das Polizeigesetz geregelt werden soll und den der Innenausschuss besonders interessiert, nämlich gegebenenfalls Software wie die von Palantir, durfte ich hier schon eingehen. Ich erkenne ausdrücklich an, dass auch aufgrund aktueller Geschehnisse das Bedürfnis der Bürgerinnen und Bürger nach Sicherheit im Zweifel gestiegen sein wird. Das will ich nicht bewerten; das ist Ihre Aufgabe. Ich nehme auch wahr, dass sich da eine Diskussion verschiebt. Ich bin aber nicht sicher, ob sich diese Diskussion gleichrangig verschiebt; denn die Polizeiarbeit wird sich aus meiner Sicht im Vergleich zu der bisherigen deutlich verändern. Aber die Sicherungsmechanismen - dazu möchte ich aufrufen; dazu hatte ich in der Stellungnahme zum Entwurf der NPOG-Novelle ausgeführt - müssen bitte mitwachsen! Versuchen Sie, bei allem Verständnis für neue Technologien, die Interessen der Bürgerinnen und Bürger im Blick zu behalten und einen vernünftigen Ausgleich zwischen den Sicherheitsinteressen und den Grundrechten insgesamt zu finden. - Mehr will ich dazu jetzt nicht sagen. Es bleibt dabei, was ich damals gesagt habe: Schaffen Sie ordentliche Rechtsgrundlagen! Man kann über vieles reden, aber das macht Arbeit.

Das nächste Thema ist ähnlich heikel und hat gleichwohl in diesem Jahr eine gewisse Renaissance erlebt: digitale Souveränität. Dieses Thema hatten wir bereits für unseren Bericht 2024 zum Startthema erhoben. Digitale Souveränität ist aus unserer Sicht kein Beschaffungsthema, sondern ein Thema, das man ständig mitdenken muss. Da fehlt es mir an Ansätzen in den IT-Konzepten des Landes. Darauf müsste ein stärkeres Gewicht gelegt werden. Dabei geht es nicht nur um „Microsoft oder nicht?“. Das fängt viel früher an, nämlich bei der Ausstattung der Arbeitsplätze, und zieht sich hin bis zu KI-Modellen. Ich ermuntere immer, das auch als Chance für den Wirtschaftsstandort Deutschland bzw. Europa zu sehen. Wir müssen nicht alles über große US-amerikanische Konzerne abwickeln. Zum Beispiel wickelt der Internationale Strafgerichtshof - aus vermeintlichem oder tatsächlichem Schaden klug geworden - künftig seinen E-Mail-Verkehr über ein Produkt ab, das über ZenDiS - eine bundeseigene GmbH - entstanden ist. Schleswig-Holstein hat sich auf den Weg gemacht, zumindest auf der ersten Ebene der Software auf Open Source umzustellen. Das alles ist ein Kraftakt und geht nicht von heute auf morgen. Aber lassen Sie uns damit anfangen! Ich glaube, das ist der richtige Weg. Ich bin weit weg, alles zu verteufeln, was es schon gibt. Die IT ist in ganz vielen Bereichen gewachsen.

Ich möchte Sie ermuntern: Seien Sie offen dafür, dass diese Dinge weitergehen! Versuchen Sie, mitzudenken, ob nicht auch Lösungen mit einem höheren Maß an digitaler Souveränität eine Lösung sein können. So kann auch ein deutscher Betreiber einer US-amerikanischen Software tätig werden, wie das beim Delos-Projekt geplant ist. Darauf kann ich später gern näher eingehen. Dieses Projekt steckt noch in den Kinderschuhen, kann aber zukünftig eine Lösung darstellen.

Zum Schluss komme ich nicht umhin, kurz die Werbetrommel zu rühren. Sie alle wissen, dass auf der Landes-, auf der Bundes- und auch auf der EU-Ebene über den Datenschutz diskutiert wird. Zu meinem großen Missvergnügen diskutiert Deutschland mal wieder nur über Strukturen, aber nicht über Inhalte. Mir wäre es wesentlich lieber, wir würden gemeinsam darüber diskutieren, an welchen Stellen wir die DSGVO weiterentwickeln müssen, wie wir uns das vorstellen. Aber hier wird über Strukturen diskutiert, zum Beispiel, ob die datenschutzmäßige Aufsicht über die freie Wirtschaft auf den Bund übergeht oder bei den Ländern verbleibt. Häufig wird der Vorwurf erhoben, die Länder seien in der Hinsicht sehr uneinheitlich. Das entspricht nicht meiner Wahrnehmung. Ich meine, die Länder versuchen sehr individuell Lösungen zu finden.

Als überzeugter Föderalist möchte ich Sie als Abgeordnete des Niedersächsischen Landtags ermuntern, diese Diskussion mitzuführen und mitzudenken, dass die Datenschutzaufsicht im eigenen Land nicht zum Schaden ist. Wir stehen in einem sehr engen Austausch, auch mit den Akteuren der Wirtschaft, und versuchen sehr kleinteilig, Lösungen zu finden und den Umgang damit zu erleichtern. Ich wiederhole mich: Es ist in der Geschichte des Landes meiner Auffassung nach nur Weniges besser geworden, wenn die Zuständigkeit beim Bund lag. Aber ich gebe zu: Das war der Werbeanteil pro domo.

Uns macht diese Aufgabe Spaß. Das Jahr hat uns viele neue tolle Einblicke verschafft. Wir machen, wenn Sie das wollen, gern so weiter.

Aussprache

Abg. **Nadja Weippert** (GRÜNE): Vielen Dank für diesen umfassenden Bericht und die damit verbundenen Einblicke.

Ich möchte auf den ersten Punkt - zur Transparenz und zum Targeting politischer Werbung - eingehen. Als Innenpolitikerin ist mir dabei ein Punkt aufgefallen, an dem wir uns in den vergangenen Jahren verändert haben, nämlich was zum Beispiel die Adressdaten von Kandidierenden angeht. Dabei geht es mir nicht so sehr um die Kandidierenden von Parteien, sondern insbesondere um Einzelkandidierende. Jetzt werden auch sie in diesem Rahmen verpflichtet, ihre Privatadresse zu veröffentlichen; denn es muss sich um eine gerichtlich ladbare Adresse handeln. Da sehe ich große Probleme, wenn ich an Hass und Hetze gegen Mandatierte denke - bis nach Hause; und das in einer Situation, in der es für uns ohnehin schwierig ist, Menschen für dieses Ehrenamt zu begeistern. In den meisten Parteien ist das so, auch in Wählergemeinschaften. Vor diesem Hintergrund frage ich, ob es noch Möglichkeiten gibt, dies generell zu heilen.

Das Ansinnen ist genau richtig. Ich finde es gut, dass die Menschen wissen können, wer wie viel in den Wahlkampf steckt, wofür die Mittel verwendet werden und woher diese stammen. Diese Transparenz brauchen wir. Ich nutze diese Möglichkeit im Wahlkampf selbst. Ich halte es für ein gutes Argument, zu sagen, dass es dazu unterschiedliche Möglichkeiten gibt; das ist nicht unbedingt ein gleicher und fairer Wettbewerb, allein schon im Hinblick auf die finanziellen Mittel. Aber an diesem von mir angeführten Punkt halte ich die Regelung für nachbesserungsbedürftig, weil er Menschen direkt betreffen kann.

LfD **Lehmkemper**: Ich habe dieses Problem wahrgenommen, aber nicht aus der eigenen Aufsichtspraxis, sondern eher als aufmerksamer Zeitungsleser. Ich habe dafür keine wirklich greifbare Lösung. Ich glaube, das muss als Problem weiterhin adressiert werden.

Lassen Sie mich anmerken: Auch wir nehmen in unserer Bearbeitung wahr, dass wir von Petentinnen und Petenten deutlich genervt und auch beschimpft werden. Insofern können wir das, was Sie beschreiben, nachfühlen. Aber ich habe keine kurzfristige Lösung. Ich nehme das Problem aber mit, und wenn die Diskussion in unserem Kreis darauf kommt, bringe ich es ein. Das sage ich Ihnen zu.

Abg. **Ulrich Watermann** (SPD): Herr Lehmkemper, Ihnen und Ihrem Team vielen Dank für den Bericht. Sie haben in Ihrem Vortrag eine ganze Reihe von Punkten angesprochen, die durchaus nachvollziehbar sind, aber das, was ich im Moment wahrnehme, nicht so richtig widerspiegeln.

Ich nehme derzeit - das haben Sie zuletzt angesprochen, das ist auch von Frau Weippert genannt worden - im Netz ein Level von Beschimpfung und Bedrohung wahr, das ich beachtlich finde. Dass sich Menschen dort in der Anonymität verbergen können, erleichtert das nach meinem Eindruck. Damit verbindet sich für mich folgende Frage: Was ist Datenschutz? Ist das ein Grundrecht? Und wie ist das im Verhältnis zu den anderen Grundrechten zu sehen - zum Beispiel meinen, wenn ich als Mensch bedroht werde? Wie gehen sie sozusagen miteinander um? Was bedeutet das eigentlich? Und ist es richtig, dass dann Täterinnen und Täter - ganz gleich, ob sie die Gewalt wirklich, in Schriftform oder wie auch immer ausüben - durch den Datenschutz geschützt werden? An der Stelle habe ich richtige Probleme.

Ich sage das so deutlich, weil ich meine, dass wir uns dieses Themas intensiv annehmen müssen; denn einige müssen diese Entwicklungen gerade ganz besonders aushalten.

Als ich 2013 im Landtag angefangen und die Verantwortung für den Bereich Innenpolitik übernommen habe, musste ich erleben, wie mein Freund Rüdiger Butte erschossen worden ist. Damals kam es gleich zu der Tat, ohne vorherige Ankündigung im Netz. Später musste ich miterleben, dass mein Freund Tjark Bartels aufgegeben hat, weil er nicht damit fertig wurde, Morddrohungen zu erhalten. Und jetzt muss ich zur Kenntnis nehmen, dass sich in meinem Umfeld viele Menschen mit so etwas auseinandersetzen müssen. Und das findet im Netz statt!

Ich glaube, dass wir ein besonderes Augenmerk auf diesen Bereich, auf den Schutz der betroffenen Menschen, legen müssen. Dazu muss es eine Abwägung geben. Das beschäftigt mich sehr intensiv, weil ich angesichts dessen, was sich da abspielt, fassungslos bin. Wenn wir in Zukunft über diese Berichte reden, müssen wir meiner Meinung nach auch diesen Komplex verstärkt in den Blick nehmen.

Ich habe noch eine Frage. Ich war etwas erschrocken und erstaunt, als ich in der Zeitung gelesen habe - auch wenn das nicht unbedingt stimmen muss -, dass die Zahl der Eingänge bei den Gerichten durch KI-Nutzung sehr stark angestiegen ist. Wie ist das bei Ihnen? Beobachten auch Sie eine solche Entwicklung, dass sich Menschen durch die KI animiert fühlen, Dinge vorzutragen, nachdem sie das vorher selbst vielleicht nicht zustande bekommen hätten? Daraus ergibt sich auch die Frage - Sie sprachen das an -, wie man dessen Herr werden soll. Mein erster und nicht ernst gemeinter Reflex war, dass dann auch die Gerichte mehr zur KI greifen müssen. Aber das halte ich für schwierig, weil ich glaube und hoffe, dass die Gerichtsbarkeit mit Menschen sympathischer zur Rechtsstaatlichkeit beiträgt als mit KI.

LfD **Lehmkemper**: Zunächst zu dem, was die Juristen „praktische Konkordanz“ nennen, also zur Grundrechteabwägung: Das Recht auf informationelle Selbstbestimmung ist ein Grundrecht - jedenfalls nach meiner festen Überzeugung. Aber es wird weder schrankenlos gewährt noch

sticht es andere Grundrechte - auch meine feste Überzeugung. Man muss also ein austariertes Verhältnis zwischen dem, was sich aus dem Datenschutz ergibt, und anderen Grundrechten erzielen. Das ist auch bei uns ein tägliches und zähes Ringen. Sie dürfen sich das nicht so vorstellen, dass ich - und schon gar nicht meine mehr als 50 Kolleginnen und Kollegen - morgens zur Arbeit kommen und sagen: Jetzt sind wir Datenschützer ohne Ende! - Herr Dr. Lahmann sagt dazu halb im Scherz: Man ist nicht nur Datenschützer, man ist auch Mensch.

Ich möchte Ihr Anliegen keinesfalls ins Lächerliche ziehen. Vielmehr macht mir das durchaus Sorgen. Denn der Satz „Datenschutz ist Täterschutz!“ stimmt nicht, aber er hat sich in unguter Weise verfestigt. Es ist viel, viel schwieriger. Neulich habe ich mit einem netten Kollegen diskutiert. Ich sagte: Spielen wir es doch mal durch und überlegen, ob eine Klarnamenpflicht im Internet - zumindest bei politischen Äußerungen - sinnvoll und praktikabel wäre. - Das klingt erstmal charmant. Wenn man früher einen Leserbrief an die Zeitung geschickt hat, musste man den Namen - oder irgendeinen Namen, jedenfalls nicht Micky Maus - drunterschreiben. Aber das Internet hat eine andere Qualität. Ich gehe auch nicht mit einem T-Shirt, auf dem meine komplette Adresse steht, durch die Fußgängerzone von Hannover. Denn dann würde ich mich vielleicht doch über Besuch von wildfremden Leuten wundern. Man muss sich das also sehr genau anschauen. Ich glaube, das ist nur in einem solchen Abwägungsprozess möglich.

Und auch wir stellen diese Problematik fest. Wir haben etliche Kundinnen und Kunden, die mir wirkliches Kopfzerbrechen bereiten. Ich schreibe regelmäßig, fast wöchentlich, Strafanzeigen. Ich zeige alles an, was in Richtung Beleidigung meiner Kolleginnen und Kollegen geht. Bei mir habe ich eine etwas höhere Schwelle. Als direkt vom Landtag Gewählter muss man da, meine ich, ein bisschen mehr aushalten. Es gibt diese Fälle, und es gab sie schon immer. Früher haben wir sie nur besser erkannt.

Als ich in der Bezirksregierung anfang, schrieben diese „Verzauberten“ - so nennen wir sie manchmal - mit der Schreibmaschine mit dem durchstechenden E rechts über den Rand. Heute sieht das alles sehr viel professioneller aus.

Das bringt mich zum nächsten Punkt: Ja, der KI-Einsatz ist gleichermaßen ein Problem und eine Chance. Die KI bietet eine Chance, weil sie es auch Menschen ermöglicht, die der Schriftsprache nicht so mächtig sind, ordentliche Texte zu verfassen; ich denke da zum Beispiel auch an Legastheniker, die formulieren, aber nur schlecht schreiben können. Das ist ein Nutzen. Aber der KI-Einsatz kann auch ein Fluch sein, wie bei so vielem. Wenn es so einfach wäre, wäre ich Anhänger der These, dass man den KI-Einsatz viel stärker regulieren muss. Aber wenn nur wir - zum Beispiel in Deutschland oder in der EU - regulieren, dann kommt am Ende auch nichts Vernünftiges heraus. Man muss also von Fall zu Fall prüfen, wie man agiert.

Aber ja, ich halte das alles für ein Problem. Aber ich halte Datenschutz *nicht* für Täterschutz. Bei vielem, zu dem ich lese, es sei wegen des Datenschutzes nicht möglich, ist es eben doch möglich - nur vielleicht nicht genau in der vorgesehenen Weise. Aber es ist möglich! Da wird Datenschutz häufig vorgeschoben und gleichzeitig zu Unrecht in Misskredit gebracht. - Gern vertiefe ich das mit konkreten Beispielen im Zwiegespräch.

Abg. **Birgit Butter** (CDU): Vielen Dank für Ihren ausführlichen Bericht. Ich habe zwei Fragen.

Zuerst eine etwas praktisch orientierte Frage: Sie haben dargestellt, dass das Fallaufkommen bei gleichbleibender bzw. zu geringer Personalstärke zunimmt. Da überrascht mich dann doch die

relativ geringe Höhe der Summe der Bußgelder von 705 000 Euro. Sie sagten, das würde einen relativ großen Fall mit über 400 000 Euro umfassen. Wie sieht es mit der Durchsetzungsfähigkeit aus? Oder sind die Fälle einfach nicht bußgeldrelevant? - Denn auch hier würde ich sagen: Arbeit muss sich lohnen. Von daher wäre ein höheres Bußgeldaufkommen schön.

Die zweite Frage ist etwas ernster. Mit ihr möchte ich Ihnen ein bisschen widersprechen. Denn in der Tat entsteht nicht nur bei Politikern, sondern auch bei Bürgerinnen und Bürgern der Eindruck, dass der Datenschutz über fast allem steht. Ich denke da an den Austausch wichtiger Daten zwischen Polizei und Behörden wie Jobcenter oder Finanzamt, der nicht erfolgen kann. Dann weiß zum Beispiel das Jobcenter nichts von dem finanziellen Status des Antragstellers. Da könnte einiges besser laufen. Insofern möchte ich Ihnen da etwas widersprechen.

Ich möchte gern Ihre Ermunterung, Rechtsgrundlagen zu schaffen, aufnehmen. Wie Sie sicherlich wissen, haben wir von der Fraktion der CDU einen Entwurf für ein Helferregistergesetz in der Pipeline, weil wir es für sinnvoll halten, dass man in einem Krisenfall weiß, wie viele Ehrenamtliche netto im Einsatz sind; denn viele Ehrenamtler sind in Personalunion an verschiedenen Stellen aktiv, zum Beispiel bei Feuerwehr und DLRG. Damit sind sie in der kritischen Infrastruktur.

Am 15. April 2026 war ich bei der Norddeutschen Sicherheitskonferenz in Bremen bei der IHK Nord. Dort äußerten die Unternehmen die Bitte, zu erfahren, welche ihrer Mitarbeiter im Krisenfall überhaupt verfügbar wären, gerade Mitarbeiter in Leitungspositionen, aber auch Lkw-Fahrer. Was macht man mit einem Reservisten, der eingezogen wird und nicht mehr die Ware von A nach B bringen kann? Dazu wurde mir gesagt, dass der Datenschutz es nicht zulässt, dass das Unternehmen erfährt, ob sich eine Arbeitnehmerin oder ein Arbeitnehmer abends noch ehrenamtlich betätigt. Was müssen wir also tun, um dorthin zu kommen? Denn ich glaube, der Datenschutz darf uns in diesen Zeiten mit ihren Bedrohungslagen nicht handlungsunfähig machen.

LfD **Lehmkemper**: Zur Bußgeldrelevanz: Natürlich ist nicht alles, was wir tun, bußgeldrelevant. Aber auf der anderen Seite ist auch klar: Wenn wir versuchen, Videofälle mit Hinweisschreiben zu befrieden, gehen uns gegebenenfalls größere Sachen durch die Lappen. Nun lautet mein Auftrag nicht, meine Behörde über Bußgelder zu refinanzieren; das hielte ich für falsch.

Was die Bußgelder angeht, versuchen wir, uns auf die wirklich bußgeldrelevanten Fälle zu kaprizieren. Wenn beispielsweise ein Unternehmen die Leistungen der Mitarbeiter anlasslos rund um die Uhr überwacht, dann kann ein Bußgeld einen sinnvollen Effekt auf die Ausgestaltung der Arbeitswelt haben; das ist unser Auftrag. Aber nicht alles ist bußgeldrelevant.

Ja, die hohen Fallzahlen führen zu Wartezeiten. Eigentlich sind wir verpflichtet, alles innerhalb von ein bis drei Monaten abzuarbeiten. Da sind wir nicht. Bisweilen sind wir bei Jahren. Je unwichtiger ein Fall ist, desto länger dauert es. Auch das halte ich für wichtig: Denn besonders relevante Fälle müssen schnell zumindest in Angriff genommen werden. Aber besonders relevante Fälle sind meist nicht sonderlich simpel, sondern binden viel Zeit. Aber natürlich sind sie oft auch spannend und insofern für die Arbeit meiner Behörde wertbildend.

Stellv. LfD **Dr. Lahmann**: Lassen Sie mich einen Maßstab für unseren Beitrag liefern. Im Jahr 2016 - also vor dem Inkrafttreten der DSGVO - betrug das höchste Bußgeld wegen einer Ordnungswidrigkeit 7 600 Euro. Die Gesamtsumme lag im fünfstelligen Bereich. In dem Bereich

bewegen sich heute Standardfälle. Wir haben also bei den verhängten Bußgeldern einen gewaltigen Sprung gemacht, um ein bis zwei Größenordnungen.

LfD **Lehmkemper**: Zum Datenaustausch zwischen Behörden habe ich eine ebenso einfache wie komplexe Antwort: Schaffen Sie Rechtsgrundlagen, wenn Sie das für politisch richtig halten! Dann werden wir im Zweifelsfall sagen, dass uns Regelungen zu weit gehen, aber Sie haben die politische Gestaltungsmacht.

Das gilt in gleiche Weise für das Helfergesetz. Ich habe mich dazu sehr lange mit der IHKN ausgetauscht und habe dazu auch aus meiner Sicht bestehende Rahmenbedingungen skizziert. Ich verstehe das Anliegen. Dabei geht es nicht nur um die Führungskräfte. Auch wenn zum Beispiel ein Staplerfahrer eines kleineren Unternehmens für zwei Tage im Rettungseinsatz war, dann funktioniert das Lager seines Unternehmens nicht mehr. Ich bin zu solchen Diskussionen bereit. Dann müssen die Daten sicher und verlässlich aufbewahrt werden.

Aber gerade im Bereich der Hilfsorganisationen kann mir doch kein Mittelständler sagen, dass er nicht weiß, wo sich seine Leute engagieren - im Gegenteil! Das ist doch eher ein Bonus als ein Malus.

Wenn wir uns gemeinsam auf den Weg machen, finden wir, glaube ich, ordentliche Lösungen, ohne dass ich schon jetzt sage, dass alles geht. Wir müssen Sie auch kritisch auf Gefahren hinweisen können. Aber Sie sind die politische Gestaltungsmacht.

Abg. **Stephan Bothe** (AfD): Sehr geehrter Herr Lehmkemper, vielen Dank für Ihren Bericht und Ihre Ausführungen. Ich habe eine Frage zu ganz aktuellen Themen, die uns bewegen. Anfang 2026 wurde das Kommunalwahlgesetz geändert. Daran waren auch Sie beteiligt; auch Sie wurden dazu angehört. Mit dieser Änderung ist es seitdem möglich, dass Wahlausschüsse oder Wahlleiter Verfassungstreueprüfungen auf Kandidaten anwenden. Die entsprechenden Voten werden im Innenministerium erfasst und den Wahlausschüssen und den Kreiswahlleitern zur Verfügung gestellt. Auf dieser Grundlage ist es zu Ausschlüssen von der Wahl gekommen; hier sind zwei davon Betroffene. Aber darum soll es hier nicht gehen. Sondern es geht darum, dass durch diese enge gesetzliche Frist Daten sofort anschließend gelöscht worden sind und Kandidaten, für die eine Verfassungstreueprüfung durchgeführt worden ist, heute über den Rechtsweg nicht mehr an diese Daten herankommen, weil das Ministerium nach der Gesetzeslage schnell gelöscht hat.

Meine Frage dazu: Handelt es sich um Datenschutz? Damit wird das ja begründet. Oder handelt es sich um Aktenvernichtung? Auch ein Kandidat, der einer solchen Prüfung unterzogen worden war, muss das Recht haben, zumindest die Daten zu prüfen, die über ihn erhoben worden sind. So ist es bei uns im Rechtsstaat eigentlich Usus. Wie bewerten Sie diesen Vorgang? Ist Ihnen dieser bekannt? Und wie würden Sie das in Zukunft besser regeln?

Vors. Abg. **Doris Schröder-Köpf** (SPD): Nach meinem Kenntnisstand ist es so, dass das Innenministerium die Unterlagen aus Datenschutzgründen nicht aufbewahrt, aber sie sind bei der Kommune und beim Verfassungsschutz vorhanden. Aber das können Sie sicherlich klären.

LfD **Lehmkemper**: Mit diesem Thema bin ich nicht im Detail vertraut. Ich beziehe mich also mehr oder weniger auf Zeitungswissen und auf das, was mir meine Kolleginnen und Kollegen freundlicherweise zur Vorbereitung recherchiert haben.

Ganz grundsätzlich sind Unterlagen nach der DSGVO dann zu löschen, wenn sie nicht mehr benötigt werden. Darum wird dann der Streit gehen. Darüber will und kann ich hier nicht entscheiden. Das ist eine Bewertungsfrage, die die Landtagsmehrheit nach meinem Eindruck so getroffen hat. Denn nach der DSGVO sind personenbezogene Daten - darum wird es gehen - dann zu löschen, wenn sie nicht mehr benötigt werden, und zwar für den Zweck, zu dem sie erhoben bzw. verarbeitet wurden.

Ich weise darauf hin, dass nach dem Kommunalwahlgesetz in aller Regel längere Aufbewahrungsfristen vorgegeben sind. Ich gehe aber davon aus - ohne dass ich mir das im Einzelnen genau angeschaut habe -, dass sich das Innenministerium zu der kurzen Löschfrist dezidiert Gedanken gemacht hat.

Von daher kann ich Ihnen jetzt weder eine fundierte Ja- oder Nein-Antwort geben, noch möchte ich an dieser Stelle gegebenenfalls anderen Verfahren vorgreifen. Aber nach dem Datenschutzrecht sind Daten zu löschen, wenn sie nicht mehr benötigt werden, und zwar bezogen auf den Zweck.

Abg. **Michael Lühmann** (GRÜNE): Vielen Dank, Herr Lehmkeper. Zu dem gerade Besprochenen reicht ein Blick ins Gesetz. Dort steht: „... unverzüglich zu löschen, sobald der Wahlausschuss den Beschluss über die Zulassung ... getroffen hat.“ - Das ist es, was die Kommunalaufsichtsbehörde zu tun hat.

(Abg. Stephan Bothe [AfD]: Das haben Sie beschlossen! Das heißt nicht, dass es richtig ist!)

Das hat der Gesetzgeber beschlossen. Gerade ging es ja um die Frage, ob das gesetzeskonform ist - und das ist es. Sie waren bei den Beratungen dabei. Wir haben das „unverzüglich“ noch aufgenommen.

(Abg. Stephan Bothe [AfD]: Ich habe dagegen gestimmt! - Gegenruf von Abg. Ulrich Watermann [SPD]: Es ist aber trotzdem mit Mehrheit vom Landtag beschlossen worden!)

- Genau.

(Abg. Stephan Bothe [AfD]: Das macht es doch nicht richtiger!)

- Aber wir diskutieren hier ja nicht über richtig oder falsch, sondern über rechtssicher.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Und jetzt läuft es bitte wieder über mich. Wer etwas sagen möchte, meldet sich bei mir.

Abg. **Michael Lühmann** (GRÜNE): Vielen Dank für den interessanten Vortrag. Ich finde das Thema immer sehr spannend, weil wir uns immer in diesem Grenzbereich befinden - gerade im innenpolitischen Bereich, wo wir gucken, was Bürger*innenrechte sind und was trotzdem wichtige Ansätze sind, um Sicherheit herzustellen. Auch ich würde nicht sagen, dass Datenschutz Täterschutz ist; auch ich finde das zu verkürzt. Vielleicht ist Datenschutz manchmal auch Aktivismusschutz oder ein Schutz vor falschen Versprechungen, was man alles tun kann.

Ich habe zwei Fragen.

Erstens. Wir wissen, dass wir bei der Novellierung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes durchaus vor einer Herausforderung stehen, was das Europarecht angeht. Sie

haben in dem Bericht ausgeführt, dass es im Omnibusverfahren Veränderungen gibt. Ich habe den Stand recherchiert. So, wie ich es verstanden habe, ist es noch nicht so ganz abgeschlossen. Aber vielleicht können Sie einschätzen, in welche Richtung es geht; denn damals haben Sie uns bei der Gesetzesberatung mitgegeben, dass wir genau diese Beratung auf der EU-Ebene im Hinterkopf haben und prüfen sollen, ob wir uns anschließen können. Was haben wir da ungefähr zu erwarten? Haben Sie einen Blick darauf, wie es aktuell steht?

Zweitens. Vor wenigen Tagen kam wieder die Debatte über die Nutzung von KI und Überwachungstechnologie hoch. Wir sehen jetzt die Debatte über die Nutzung der Brillen von Meta und anderen, mit denen man in der Öffentlichkeit als Brillenträger dauerhaft Aufnahmen machen kann. Dann wurde darauf hingewiesen, dass sich daran eine kleine rote Kontrollleuchte befindet, womit alles in Ordnung sei. Ich stelle es mir schwierig vor, in großen Menschenansammlungen zu schauen, bei wem gerade eine Kontrollleuchte rot aufleuchtet.

Wenn man das mit Berichten zusammennimmt, dass von verschiedenen Akteuren - bis hin zu Sicherheitsbehörden - Standortdaten gekauft werden und in den USA im Zweifelsfall alles zusammengeführt wird, was man zusammenführen kann, ergibt sich eine besondere Qualität. Haben Sie einen Blick auf den Umgang mit diesen KI-Brillen? Denn im Prinzip kann damit jeder die Daten für die Verfolgungsinteressen von allen möglichen Akteur*innen liefern. Da reden wir nicht nur über demokratische Player, sondern auch über einen Donald Trump, der durchaus Interesse hat, bestimmte Gruppen zu verfolgen. Und wie soll man damit umgehen, wenn Bürgerinnen und Bürger bewusst oder unbewusst über ihre KI-Brillen Daten liefern? Wie ist der Blick darauf? Wir stehen ja am Anfang. Eine Einschätzung wäre interessant.

LfD **Lehmkemper:** Was die Omnibus-Gesetzgebung in der EU angeht, bin ich nicht mehr ganz so optimistisch wie im Frühsommer, zumal die NPOG-Novelle in die JI-Richtlinie hineinragt, die auf der EU-Ebene nicht diskutiert wird, allenfalls über KI.

Was Erleichterungen angeht, schält sich heraus, dass über die Änderung von Artikel 88 c entsprechend der aktuellen Entwurfsfassung für die öffentliche Hand Erleichterungen herbeigeführt werden sollen. Die Diskussion, ob das auch für den Sicherheitsbereich gelten kann oder soll oder muss, habe ich bislang nicht wahrgenommen. Trotzdem empfehle ich, einen Blick darauf zu haben. Ich sage zu, dass wir das weiterhin im Blick haben werden.

Ein wesentlicher Punkt in unserer Stellungnahme war auch, dass die Verfahren, die dahinter stecken, zwar polizeiliche Wünsche abbilden, aber noch nicht konkret genug beschrieben waren, um auf dieser Grundlage eine Norm abzubilden. Ich verstehe das Problem, dass man eine solche Norm nicht nur für den einen Anwendungsfall erstellt. Das ist auch eine rechtliche Errungenschaft. Aber es ist dann besonders schwierig, wenn man nicht so recht weiß, was mit den Verfahren gemacht werden soll. Da sind wir uns sicherlich einig.

Ja, weiter darauf blicken! Wir tun das. Lassen Sie es uns so machen: Wenn Sie Nachbesserungs- oder zusätzlichen Informationsbedarf haben - gern! Das erscheint mir seriöser, als wenn ich wie jetzt gerade fabuliere.

Was die Meta-Brillen angeht, bin ich, offen gestanden, ein bisschen zwiegespalten. Natürlich kann das ein hochpotentes Überwachungsinstrument sein - keine Frage! Aber davon gibt es sehr viele. Wollen wir das alles wirklich verbieten? Ich sehe auch den Nutzen dieser Brillen und würde mir eher wünschen, meine Behörde wäre so ausgestattet, dass ich Fehlgebräuche sanktionieren

könnte. Das ginge dann in die Richtung der Äußerung von Frau Butter: Das wären wichtige Themen, derer wir uns annehmen könnten.

Ich gebe Ihnen ein Beispiel für den praktischen Nutzen: Ich fotografiere gern, auch um Fotobücher zu erstellen. Nach einem Sturz mit einem komplizierten Knochenbruch war ich, weil ich auf zwei Gehhilfen angewiesen bin, aber nicht mehr in der Lage, im Stehen mein Handy für ein Foto aus der Tasche zu ziehen. Eine solche Brille gibt jemandem, der die Hände im Stehen nicht frei hat, die Möglichkeit zu fotografieren. Eine solche Brille gibt jemandem, der nicht gut sieht, die Möglichkeit, sich beschreiben zu lassen, was in seinem Blickfeld ist, aber für ihn nicht erkennbar ist.

Außerdem geht es um den Selbstschutz: Man kann bei solchen Brillen einstellen, dass Meta die Daten nicht erhält, hat dann aber auch weniger Komfort.

Ich bin, wie bei vielem, für eine differenzierte Betrachtung. Aber wir stehen ganz am Anfang dieser Diskussion. Ich bin mir durchaus der Tatsache bewusst, dass der innerhalb Deutschlands zuständige Kollege aus Hamburg dazu eine sehr viel rigorosere Meinung als ich vertritt.

Abg. **Evrin Camuz** (GRÜNE): Vielen Dank Ihnen und Ihrem Team für den Bericht, Herr Lehmkemper.

Erstens. Es passt gut, dass wir gerade über Smart Glasses sprechen. Wir sehen sie mittlerweile in der privaten Nutzung. Ab Seite 81 berichten Sie über einzelne Bußgeldverfahren. Jetzt gibt es auf TikTok und Instagram das Phänomen, dass - fast ausschließlich - Männer unter den Hashtags #rizz und #pickupartist Frauen filmen, ohne dass diese es mitbekommen, weil die Brillen so manipuliert sind, dass man keine Kontrollleuchte sieht. Vielmehr sehen diese Smart Glasses wie eine typische und verbreitete Ray-Ban-Brille aus.

Sie haben zu Recht darüber informiert, dass es im Rahmen der praktischen Konkordanz immer um eine Grundrechtsabwägung geht; das ist selbstverständlich. Wir haben hier auf der einen Seite das Recht auf informationelle Selbstbestimmung und auf der anderen Seite die Kunst- oder Meinungsfreiheit. Überlegen Sie in Ihrem Team, Kontakt mit der Stiftung Opferhilfe aufzunehmen, ob es Möglichkeiten gibt, Betroffenen - fast ausschließlich Frauen - irgendwie Hilfe anzubieten, wie damit umzugehen ist und wie das Recht auf informationelle Selbstbestimmung umgesetzt werden kann? Denn viele sind ratlos. Wir haben dieses Phänomen zunächst in den USA gesehen, und jetzt passiert das auch in Deutschland. Für mich ist das eine Form der digitalen Gewalt.

Mittlerweile liegt der erste Entwurf der Bundesjustizministerin, Frau Hubig, vor, mit dem diverse Rechtsschutzlücken geschlossen werden sollen; das finde ich gut. Aber dieses Phänomen ist nicht abgebildet - das ist schwierig; denn es liegt in der Natur der Sache, weil es so oft neue Phänomene gibt. Vielleicht kann schon mit Flyern geholfen werden; denn die Nachfrage danach kommt, und ich fände es ärgerlich, wenn man jetzt auf diverse Verfahren warten müsste.

Zweitens. Netterweise geben Sie zu Beginn Ihres Berichts auch immer Empfehlungen an die Landesregierung und an das Parlament. Fast alle Empfehlungen betreffen den Justizbereich. Ich hatte bereits um eine Information gebeten, wie das Justizministerium dazu steht. Ich warte noch auf eine Antwort. Aber vielleicht stehen Sie im Austausch. Mich interessiert, ob Sie diesbezüglich bereits im Kontakt mit der Landesregierung bzw. mit dem Justizbereich sind.

Drittens. Wir haben gerade über diverse Täter im Internet gesprochen, die dort sehr viel Hass und Hetze verbreiten; Herr Watermann hatte das Thema eingebracht. Ich beobachte, dass hinter diesen Postings Bots stehen, also keine Menschen. Wer übernimmt dafür die Verantwortung? Der Benutzer dieser App, der nicht vorgegeben hat, dass diese Person so und so zu beleidigen ist, sondern die App über Schlüsselwörter so programmiert hat, dass gefiltert und darauf kommentiert wird? Beispielsweise beim Stichwort „Klima“ werden also entsprechende Bemerkungen angefügt. Oder müssen wir, wie so oft, die Unternehmen angehen?

LfD **Lehmkemper**: Um es klar zu sagen: Was das #rizz-Phänomen angeht, stehen wir nicht im Kontakt mit Stiftungen, auch nicht mit der Stiftung Opferhilfe. Der Weg ist ganz einfach: Das sind Videofälle neuer Qualität. Das ist Videoüberwachung oder unvermutetes Fotografieren. Da ist nach der DSGVO die Beschwerde bei uns das Mittel - online, per Mail, ganz niedrigschwellig.

Uns liegen solche Fälle noch nicht vor. Ich hatte das abgefragt. Wenn wir solche Fälle hätten, würden wir uns das sehr genau anschauen; denn nach meiner heutigen Wertung ist der Unrechtsgehalt der Tat deutlich höher als bei einer um 5 Grad falsch justierten Videokamera, die eigentlich nur das eigene Grundstück filmen soll. Ich glaube, da werden wir uns sehr schnell einig.

Also ermuntern Sie bitte jede und jeden, die Möglichkeiten der DSGVO zu einer Beschwerde zu nutzen. Wir werden uns das anschauen - trotz der hohen Fallzahlen bei uns. Wir haben allerdings - auch das will ich sehr deutlich sagen - eine sehr hohe Akzeptanz von allem, was aus der Privatwirtschaft kommt. Die Wellen laufen immer relativ schnell hoch auf, wenn der Staat irgendetwas in Richtung „Daten“ insgesamt macht. Aber dass das eigene iPhone viel besser als der eigene Ehepartner weiß, wo man sich gerade aufhält, haben wir alle seit vielen Jahren akzeptiert. Das ist ein zusätzliches Problem. Aber ermuntern Sie gern dazu, die Mittel der DSGVO zu nutzen!

Sollte das zum verbreiteten Phänomen werden - wir gehen in der Öffentlichkeitsarbeit ohnehin häufig mit FAQs um und haben auf unserer Website in letzter Zeit viel gemacht -, werden wir das sicherlich aufgreifen. Aber so weit ist es nach meinem Eindruck noch nicht.

Antworten der Landesregierung auf unsere Berichte - früher habe ich selbst bei der Abfassung solcher Antworten mitwirken dürfen - sind bisweilen ja auch Pflichtübungen. In der niedersächsischen Initiative „Einfacher. Schneller. Günstiger.“ will man die Pflicht, auf unsere Berichte zu antworten, auch noch streichen. Aus der Sicht des Bearbeiters kann ich das verstehen. Für Sie finde ich es schade; denn Sie bekamen und bekommen von meinen Vorgängern und mir einen recht ausführlichen Bericht, zu dem wir uns austauschen. Aber zum Austausch mit den relevanten Gremien in den Ressorts kommt es nicht. Die Streichung der Pflicht, den Bericht der oder des LfD zu beantworten, wird ihn noch mehr zu einem singulären Phänomen machen. Aus der Sicht des Bürokratieabbaus ist das aber verständlich. Sie müssen dann bewerten, ob es vernünftig ist, dass keine Erwiderung stattfindet.

Was die Bots im Internet angeht: Derjenigen, die hinter ihnen stehen, muss man erst einmal habhaft werden! Ganz häufig haben diejenigen, die die Bots programmiert haben, ihren Sitz nicht im Einflussbereich der DSGVO. Von daher kann ich diese einfache Antwort geben: Mir wäre sehr viel wohler, wenn die Europäische Kommission als die in sehr vielen Fällen Zuständige die Plattformen schärfer unters Regime nehmen würde. Nach meiner Ansicht gehört auch das in den heute schon beschriebenen Phänomenbereich der Verrohung im Internet.

RefL **Bölsing** (LfD): Ich habe die Fragestellung so verstanden, dass es um unsere Empfehlungen an Sie geht, die im Tätigkeitsbericht enthalten sind. Darin sind zwei Empfehlungen in Richtung des Justizministeriums enthalten. Ich darf darauf kurz eingehen.

Die erste Empfehlung betrifft die Aufsicht über die justizielle Tätigkeit. Es ist richtig, dass uns die DSGVO keine Aufsichtsmöglichkeit gibt; denn das gebieten der Rechtsstaat und die Gewaltenteilung. Darum pflegen wir bereits seit ungefähr 2020 einen engen Austausch mit dem MJ und fordern, wie es auch die DSGVO und die JI-Richtlinie vorsehen, dafür besondere Stellen in der Justiz zu schaffen. Denn wenn sich ein Mensch über das Verhalten einer Richterin oder eines Richters beschwert, beschwert er sich bei uns, aber wir können nur auf die fehlende eigene Zuständigkeit verweisen und darum bitten, sich an das MJ zu wenden. Von dort wurde bisher stets keine Erforderlichkeit gesehen, weil man ja die normalen prozessualen Möglichkeiten habe, gegen derartige Dinge vorzugehen. Das ist aber aus meiner Sicht zu kurz gegriffen, weil ja gerade die DSGVO, die auch für die Justiz gilt, entsprechende weitere Möglichkeiten außerhalb der normalen prozessualen Vorgänge schafft. Dementsprechend haben wir das zum einen auf dem Kanal der direkten Ansprache des MJ und zum anderen auf dem Kanal der Datenschutzkonferenz adressiert. Dort gibt es unter anderem einen Arbeitskreis Justiz. Auch dort hat man dieses Problem gesehen. Von dort wurde das Problem der Justizministerinnen- und -ministerkonferenz vorgetragen. Aber auch dort wurde beschrieben, dass eine entsprechende Änderung nicht erforderlich sei. - Das ist der momentane Stand zur Behebung dieser Lücke in der aufsichtsrechtlichen Zuständigkeit.

Die zweite Empfehlung betrifft die Zuständigkeit in Bußgeldverfahren; das ist nicht originär meine Zuständigkeit. Aber dazu gibt es keinen neuen Stand gegenüber dem MJ, wie mir die zuständige Kollegin gerade versicherte. So, wie ich es verstanden habe, gab es einen Austausch und eine Forderung, aber das ist bislang seitens des MJ nicht aufgegriffen worden.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Mir liegen noch vier Wortmeldungen vor. Die arbeiten wir noch ab, und dann möchte ich in Anbetracht der restlichen Tagesordnung zum nächsten Punkt kommen.

Abg. **Alexander Saade** (SPD): Vielen Dank für Ihren kurzweiligen Vortrag.

Vorhin ging es kurz um eine mögliche Klarnamenpflicht im Internet. Dazu möchte ich Sie um eine Einschätzung bitten. Für mich wäre eine Klarnamenpflicht eher eine Pflicht, sich gegenüber dem Betreiber zu identifizieren. Aber aus meiner Sicht steht nichts der Möglichkeit entgegen, dass man im Internet weiterhin mit einem Pseudonym unterwegs ist. Dann hätten Strafverfolgungsbehörden möglicherweise einen direkten Zugriff über den Anbieter auf den Tatverdächtigen. Wie würden Sie das einschätzen?

LfD **Lehmkemper**: Das klingt auf den ersten Blick charmant, hat aber natürlich zur Folge, dass all die Betreiber - unter anderem Elon Musk - über alle Klarnamen verfügen würde.

Ich finde, an diesem Beispiel wird deutlich, wie komplex das Thema ist. Ich glaube bei Beobachtung derer, die es betrifft: Das Instrument würde ins Leere laufen, weil es viele geben würde, die nicht bereit wären, Elon Musk zu sagen, wie sie heißen. Ob die dann aber nicht mehr im Internet aktiv sind oder nicht doch über irgendwelche VPN-Verschlüsselungen, mehr oder weniger obskure Browser oder über irgendwelche anderen Wege Ähnliches tun, weiß ich nicht. Das

zeigt meiner Meinung nach exemplarisch, wie schwierig die Umsetzung ist. Ich glaube auch, dass man das europaweit regeln muss, aber auch, dass nicht alles möglich ist.

Wir werden diese gesellschaftliche Diskussion zu führen haben: Will ich weiterhin hinnehmen, dass im Netz diese Art von Gewalt - ja, das sehe auch ich so - zunimmt und die Auseinandersetzungen so geführt werden? Oder will ich das über Maßnahmen gegen die Plattformen und über andere Möglichkeiten einschränken? Aber das wird dann ein Stück weit das Internet - zumindest diesen Teil des Internets - verändern. Das ist dann nicht mehr mein Job, sondern Ihrer.

Abg. **André Bock** (CDU): Vielen Dank, Herr Lehmkemper, für Ihren Bericht. Der heutige Vormittag zeigt wieder deutlich, dass es gut ist, dass wir Sie und Ihr Team dort haben, wo wir Sie haben. Sie leisten eine wirklich gute Arbeit in einem Bereich, der vielleicht nicht immer so im Fokus der Öffentlichkeit steht wie manche Taten, zum Beispiel wie die Tat vor wenigen Wochen in Stade, aber doch sehr wichtig ist, weil Probleme im Bereich Datenschutz jeden auf dem ganzen Globus in seiner persönlichen Sphäre betreffen können. Insofern vielen Dank für Ihre Arbeit.

Ich habe drei Bitten oder Appelle an Sie, Herr Lehmkemper.

Erstens. Sie tragen wie auch heute immer wieder bescheiden vor, was Sie mit Ihrem Team alles abarbeiten, wie die Fallzahlen gestiegen sind und mit welchen Fällen Sie sich beschäftigen; das können wir im Detail nachlesen. Am Rande werden dann die Stichworte „Personal“ und „Personalbesatz erhöhen“ angedeutet. Fordern Sie durchaus, was Sie benötigen! Wir alle müssen hier darüber sprechen, dass wir für die Zukunft aufrüsten, weil die Bedeutung dieses Bereichs und die Zahl der Fälle immer weiter zunehmen werden. Seien Sie also nicht so bescheiden!

Zweitens wird man auch über die Frage sprechen müssen, welche Fälle Sie bearbeiten. Sie haben den Dash-Cam-Fall erwähnt. Das ist bei einer großen Sicht vielleicht eine Bagatelle, wenn auch für den Einzelnen sicherlich nicht. Man könnte das mit der Arbeit der Polizei und der Ordnungsbehörden vergleichen: Es werden Knöllchen fürs Falschparken geschrieben - und dahinter steht ein immenser Verwaltungsaufwand -, und gleichzeitig gibt es ganz andere große Fälle vor Ort. Darüber wird noch zu sprechen sein.

Drittens ist deutlich geworden, wie komplex alles rund um Datenschutz, Datensicherheit einerseits ist, aber andererseits auch, wie komplex alles rund um das Datenbedürfnis unserer Sicherheitsbehörden ist. Sie haben in Ihrer Einleitung angedeutet, an welchen Stellen Sie es besser fänden, wenn die Länder und nicht der Bund zuständig wären. Weil wohl alle Parlamentarier derartige Vorträge hören - Landtage, sicherlich auch der Bundestag -, möchte ich die Idee ins Spiel bringen - in der Hoffnung, dass so etwas bislang nicht an mir vorbeigegangen ist -, alle ein oder zwei Jahre eine Art von Symposium mit allen Datenschutzbeauftragten und den Mitgliedern der Innen- und Rechtsausschüsse der Länder abzuhalten, um sich über diese Themen auszutauschen. Dann kann es auch um die Rechtsgrundlagen gehen, zu deren Anpassung oder Bereitstellung Sie heute mehrfach aufgerufen haben. Aber auch das Technische muss damit einhergehen; denn die Technik für unsere Sicherheitsbehörden muss mitlaufen. Aber dort könnte man sich auch über spezielle Fälle, wie sie heute angesprochen worden sind, austauschen.

Lasst uns doch mal länderübergreifend mit den Innen- und Rechtspolitikern zusammensetzen, damit wir uns über diese Themen austauschen und auch abgleichen können, was welches Bundesland wie macht! Denn ich glaube nicht, dass es hier einen Überblick gibt, was in den anderen Ländern besonders gut läuft oder wo Initiativen für ein gemeinsames politisches Agieren

bestehen. Die Aufgaben des Datenschutzes - auch zu allem, was mit KI zu tun hat - werden zunehmen und uns als Gesellschaft und Politik massivst herausfordern.

Vielleicht kann eine Einladung zu einem solchen Symposium unter Einbeziehung von Landesinnen- und -rechtspolitikern von den Datenschützern ausgehen. Dann könnte man sich auch in aller Ruhe und nicht nur an einem halben Vormittag zu diesen wichtigen Themen austauschen.

Abg. **Nadja Weippert** (GRÜNE): Zur Klarnamenpflicht: Auch wenn sich jemand über den Betreiber ermitteln ließe - es geht eher um die Anonymität bzw. ihr Ende. Wenn zum Beispiel Heinz Müller in der Facebook-Ortsgruppe etwas unter seinem eigenen Namen schreibt, dann sehen und wissen das auch andere. Deshalb ist die Hemmschwelle, etwas Aggressives etc. zu schreiben, unter Anonymität niedriger. Von daher halte ich es nicht für sehr zielführend, den Klarnamen nur gegenüber dem Betreiber anzugeben.

In diesem Zusammenhang spielt auch die Dauer der Bearbeitung derartiger Strafanzeigen eine Rolle. Selbst wenn solche Strafanzeigen gestellt werden, ist die Bearbeitungsdauer tendenziell zu lang, um Wirkung zu zeigen. Im vergangenen Jahr hatte ich es mit einer anonymen E-Mail mit wirklich heftigen Bedrohungen zu tun. Die dafür verwendete anonyme E-Mail-Adresse musste, wie ermittelt wurde, über eine Telefonnummer registriert werden. So kam nach drei Monaten der Name des Tatverdächtigen heraus, der aber alles abstritt. Eine so lange Zeit ist nicht hinzunehmen.

Die Justizministerin hatte 2025 zu einem Symposium „Hass im Netz“ ins Gästehaus der Landesregierung eingeladen. Dabei wurde deutlich, dass das Schlimmste eigentlich ist, nach solchen Anzeigen entweder gar keine Rückmeldung zu bekommen oder sehr lange darauf warten zu müssen. Mittlerweile ist die Aufklärungsquote trotzdem ziemlich hoch; ich meine, es war im vergangenen Jahr von 80 % gesprochen worden. Der Schutz der Anonymität ist also nicht mehr unbedingt gegeben - aber es geht darum, solche Taten im Keim zu ersticken. Und wenn jemand so etwas mit seinem Klarnamen sagen möchte, ist die Hemmschwelle wesentlich höher, weil sich die Person gegebenenfalls vor den Nachbarn beim Einkaufen rechtfertigen muss. Darin sehe ich den entscheidenden Punkt, was eine Klarnamenpflicht angeht.

Ich möchte aber noch ein anderes Thema ansprechen, nämlich VW. Sie hatten vorhin, als es um Prioritäten und Bearbeitungsdauern ging, von den großen Themen angesprochen. Wie ist der Sachstand zum VW-Datenskandal von Ende 2024 und dem Tracking der Fahrzeuge?

LfD **Lehmkemper**: Wir stehen seit diesem Vorkommnis im intensiven Austausch mit VW bzw. der betroffenen Tochtergesellschaft. Es handelt sich dabei um eine Datenpanne, deren technische Aufarbeitung - es ging um Lastspitzen bei der Cloudnutzung - extrem kompliziert war. Ich bin froh und dankbar, dass ich über ein auch in technischen Fragen so engagiertes Team verfüge.

Wir haben mehrfach und intensiv versucht, schon im Vorfeld eines Bußgeldverfahrens eine gütliche Einigung herbeizuführen; es ging um die Zahlung einer, wie wir finden, angemessenen Verständigungsgeldbuße. Mittlerweile haben wir das Bußgeldverfahren eingeleitet und hören das betroffene VW-Tochterunternehmen im Bußgeldverfahren an.

Sie alle wissen, dass Bußgelder für Datenschutzbehörden ein heikles Thema sind. Auf der einen Seite sind wir durch den Europäischen Datenschutzausschuss gebunden, der eine Bußgeldskala aufgerufen hat, die völlig inkompatibel mit der Bußgeldrechtsprechung deutscher Gerichte ist. Ich will auf keinen Fall das Zeichen setzen: Ihr müsst nur gegen meine Bescheide klagen, und

schon müsst ihr nur 20 oder 25 % des von mir verhängten Bußgelds zahlen. - An der Stelle bin ich nämlich trotz aller rechtlicher Unabhängigkeit durch das Europarecht gebunden und werde durch die anderen Aufsichtsbehörden kontrolliert. Ich mache es mal plastisch: Ich muss immer damit rechnen, dass sich die französische Aufsichtsbehörde - auch in Frankreich gibt es eine bedeutende Autoindustrie - anschaut, wie der niedersächsische LfD VW behandelt.

In diesem sehr konstruktiven Austausch stehen wir im Moment auf zwei unterschiedlichen Seiten und haben uns - für VW nicht überraschend - dafür entschieden, ins Bußgeldverfahren zu gehen. Nach Eingang der Stellungnahme zu diesem Bußgeldverfahren werden wir uns über die Bußgeldhöhe Gedanken machen. - Ja, das hat sehr lange gedauert, Herr Dr. Lahmann und sein Team hatten da auch ein dickes Brett zu bohren.

Abg. Thorsten Paul Moriße (AfD): Vielen Dank für Ihren Vortrag, Herr Lehmkemper. Sie erwähnten, dass Sie sich schützend vor die Mitarbeiter Ihrer Datenschutzbehörde stellen; das ist auch gut so.

Aber ich frage Sie einfach mal umgekehrt: Das Verwaltungsgericht Oldenburg hat mögliche Verstöße gegen Datenschutzvorschriften und Persönlichkeitsrechte in Verfahren wie in meinem - es geht noch einmal um den Wahlausschluss - im Visier. Deswegen wurden sämtliche Unterlagen durch das Verwaltungsgericht angefordert. Wie stellen Sie sicher, dass Datenschutzverstöße durch staatliche Stellen wie die Wahlausschüsse, die solche Verfahren betreuen, konsequent aufgeklärt und sanktioniert werden? Welche konkreten Maßnahmen ergreifen Sie, wenn das Verwaltungsgericht Oldenburg Hinweise auf erhebliche Rechtsverstöße liefert?

Und sind Sie vom Verwaltungsgericht schon irgendwie in diesem Kontext aufgefordert worden?

LfD Lehmkemper: Natürlich gehen wir auch Verstößen der öffentlichen Stellen in Datenschutzfragen nach. Nach dem deutschen Recht steht uns ein anderer Kanon von Maßnahmen zur Verfügung. Wir dürfen gegen öffentliche Stellen keine Bußgelder verhängen; ich halte das für nachvollziehbar und kann bei Bedarf anhand eines Musterfalls begründen, warum ich das für korrekt halte. Das wird in der Datenschutz-Community allerdings durchaus kritisch gesehen.

Ich bin eine Verwaltungsbehörde. Wenn ein Gericht entscheidet, habe ich im Grunde nichts mehr zu tun; denn dann hat es über den Rechtsverstoß entschieden, was häufig dazu führt - ich spreche jetzt allgemein, nicht mehr zu Ihrem Fall, weil ich ihn nicht kenne -, dass wir bei derartigen Sachverhalten mitteilen: Wenn parallel zur Beschwerde bei uns ein Gericht damit befasst ist, dann soll das Gericht agieren. Das hat etwas mit Gewaltenteilung zu tun, dann hat sich die Verwaltungsbehörde zurückzuhalten. Sollte dann noch ein Überhang bestehen, der datenschutzrechtlich zu bewerten wäre - wie auch immer; ich kann mir das gerade nicht so recht vorstellen -, müssten und würden wir uns das anschauen. Das kann dann bis zur Beanstandung eines Vorfalls gegenüber einer öffentlichen Stelle gehen.

Verfahrensfragen

Abschließend kommen beide **Ausschüsse** überein, künftig den Bericht des Landesbeauftragten für den Datenschutz regelmäßig in gemeinsamer Sitzung entgegenzunehmen.

LfD **Lehmkemper** wirbt dafür, den jährlichen Tätigkeitsbericht in Zukunft wieder vor der Sommerpause des Folgejahres entgegenzunehmen.
